В. М. БОГУШ, В. Д. БРОВКО, О. С. КОБУС, В. Д. КОЗЮРА

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ:
теоретичні основи та організаційно-технічне забезпечення

Навчальний посібник

Київ
Видавництво Ліра-К
2023

УДК **004.056.5**
Т38

Рецензенти:

Мамченко С. М., доктор педагогічних наук, професор;
Хорошко В. О., доктор технічних наук, професор

Т38 **Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення.** Навч. посіб. / В. М. Богуш, В. Д. Бровко, О. С. Кобус, В. Д. Козюра: під. ред. В. М. Богуша. К.: Видавництво Ліра-К, 2023. — 484 с.

ISBN 978-617-520-642-3

У навчальному посібнику наведена систематизована сукупність відомостей, що забезпечує з'ясування понять захисту інформації з обмеженим доступом, як однієї з найважливіших сфер діяльності держави, опанування основними термінами та категоріями технічного захисту інформації на рівні їх тлумачення і відтворення для практичного застосування та втілення у процесі фахової та професійної діяльності із забезпечення національної безпеки в інформаційній сфері та кіберпросторі.

Розрахований на курсантів, слухачів та студентів закладів вищої освіти, які навчаються за всіма освітніми програмами спеціальностей 125 Кібербезпека та захист інформації і 256 Національна безпека (за окремими сферами забезпечення і видами діяльності). Може бути корисним широкому колу керівників і працівників служб безпеки державних та комерційних організацій.

УДК 004.056.5

ISBN 978-617-520-642-3

ЗМІСТ

ВСТУП

Навчальний посібник відображає сучасні погляди на стан розвитку теорії і практики технічного захисту інформації з обмеженим доступом.

Причому, основні визначення дисципліни сформульовані відповідно до законодавчих актів України [53]:

— технічний захист інформації — це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особистості, суспільства і держави;

— система технічного захисту інформації — це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

Особливого значення технічний захист інформації набуває як один із основних напрямів кіберзахисту в системах забезпечення кібербезпеки [48], а також у забезпеченні безпеки об'єктів критичної інфраструктури [48; 106].

У **першій частині** посібника наведені основні положення системного підходу щодо захисту інформації, загальних концептуальних підходів щодо побудови системи технічного захисту інформації в державі і в організації, характеристик інформації як предмета захисту, загроз безпеці інформації та методів технічного захисту інформації.

У **другій частині** посібника розглядаються особливості організаційного та методичного забезпечення системи технічного захисту інформації, основи побудови системи і основних підсистем технічного захисту інформації, що включає: типовий підхід до побудови системи технічного захисту інформації організації, який включає застосування засобів технічної охорони об'єктів, засобів протидії спостереженню і підслухуванню, засобів попередження витоку інформації через побічні електромагнітні випромінювання і наведення.

Посібник містить також словники додаткових термінів і понять, одиниць вимірювання та покажчик ключових термінів і понять. Ключові тер-

міни і поняття технічного захисту інформації, які формулюються у основному тексті посібника та у словнику додаткових термінів і понять, виділені жирним шрифтом. Наведені також англійські еквіваленти термінів і понять, а також їхня етимологія, тобто визначення походження слова шляхом співставлення його зі спорідненими словами тієї або іншої мови. Це дозволяє досить докладно окреслити предметну частину технічного захисту інформації та використовувати посібник як тлумачний словник.

Автори висловлюють щиру вдячність рецензентам: доктору педагогічних наук, професору С. М. Мамченку та доктору технічних наук, професору В. О. Хорошку за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

Особливу вдячність автори висловлюють генеральному директору науково-впроваджувальної фірми «Криптон» О. Й. Куляниці за плідні дискусії та цінні поради, що сприяли появі посібника та формуванню його змісту.

ПЕРЕЛІК АБРЕВІАТУР

Україномовні

АТС	—	автоматична телефонна станція
БД	—	база даних
БЗ	—	база знань
БПЛА	—	безпілотний літальний апарат
ДК	—	дозиметричний контроль
ДПЛА	—	дистанційно пілотований літальний апарат
ДРР	—	дешифрувально-розвідувальна робота
ДТЗС	—	допоміжний технічний засіб і система
ЕОТ	—	електронно-обчислювальна техніка
ЕПР	—	ефективна площа розсіювання
ЕРС	—	електрорушійна сила
ІПС	—	ізольоване програмне середовище
ІС	—	інформаційна система
ІТС	—	інформаційно-телекомунікаційна система
ЗОТ	—	засіб обчислювальної техніки
ЗТО	—	засіб технічної охорони
КЛА	—	космічний літальний апарат
КОПС	—	комплекс охоронно-пожежної сигналізації
КПП	—	контрольно-пропускний пункт
ЛА	—	літальний апарат
МДН	—	метал-діелектрик-напівпровідник
НСД	—	несанкціонований доступ
ОПР	—	особа, що приймає рішення
ОС	—	операційна система
ОТЗ	—	основний технічний засіб
ПАКСЗІ	—	програмно-апаратний комплекс системи захисту інформації
ПВЧ	—	підсилювач високої частоти
ПЗ	—	програмне забезпечення
ПЗЗ	—	прилад із зарядовим зв'язком
ПКП	—	приймально-контрольний прилад
ПЕМВН	—	побічні електромагнітні випромінювання і наведення
ПЕОМ	—	персональна електронно-обчислювальна машина
ПЗП	—	постійний запам'ятовуючий пристрій
ПНБ	—	прилад нічного бачення
ПНЧ	—	підсилювач низької частоти
ППЧ	—	підсилювач проміжної частоти

ПРД	—	правило розмежування доступу
ПЦС	—	пульт централізованого спостереження
РЕБ	—	радіоелектронна боротьба
РЕЗ	—	радіоелектронний засіб
РЛС	—	радіолокаційна станція
СКУД	—	система контролю управління доступом
СД	—	спеціальне дослідження
СЕП	—	спеціальний електронний пристрій
СО	—	спеціальне обстеження
СП	—	спеціальна перевірка
ТЗІ	—	технічний захист інформації
ТТХ	—	тактико-технічна характеристика
ШСЗ	—	штучний супутник Землі

Англомовні

ACOUSINT	—	ACOUStic INTelligence
BIOS	—	Basic Input/Output System
DNS	—	Domain Name System
DOS	—	Disk Operating System
CDMA	—	Code Division Multiple Access
CCD	—	Charge-Coupled Device
COMINT	—	COMmunications INTelligence
FDD	—	Floppy Disk Drive
EASI	—	Estimate of Adversary Sequence Interruption
EDGE	—	Enhanced Data rates for Global Evolution
ELINT	—	ELectronic INTelligence
ISO	—	International Organization for Standardization
MISFET	—	Metal Insulator-Semiconductor Field-Effect Transistor
NUCINT	—	NUClear INTelligence
OSINT	—	Open Source INTelligence
POST	—	Power-On Self-Test
RADINT	—	RADar INTelligence
RPV	—	Remotely Piloted Vehicle
SCSI	—	Small Computer Systems Interface
TM	—	Touch Memory
WEP	—	Wired Equivalent Privacy
WLAN	—	Wireless Local Area Network
WMAN	—	Wireless Metropolitan Area Networks
WPA	—	Wi-Fi Protected Access
WPAN	—	Wireless Personal Area Network

Частина I

Основи технічного захисту інформації

Розділ 1

Системний підхід до технічного захисту інформації

1.1. Основні положення системного підходу до технічного захисту інформації

Сформувати уявлення про комплекс завдань щодо побудови системи технічного захисту інформації, методів, заходів і засобів для її реалізації на об'єктах інформаційної діяльності організації найбільш доцільно на основі системного підходу [3; 130].

Системний підхід [systems approach] — це дослідження об'єкта або процесу за допомогою моделі, званою системою. Цей підхід передбачає найвищий рівень опису об'єкта дослідження — системний. Найнижчим рівнем є рівень опису параметрів об'єкта — параметричний. Між ними розташовуються структурний і функціональний рівні (рис. 1.1).

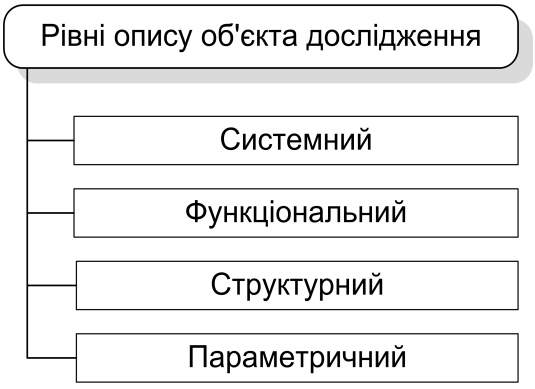

Рис. 1.1. Рівні опису об'єкта

Сутність системного підходу полягає в наступному:

— сукупність сил і засобів, які забезпечують вирішення завдання, представляється у вигляді моделі, званою системою;
— система описується сукупністю параметрів;
— будь-яка система розглядається як підсистема більш складної системи, що впливає на структуру і функціонування розглянутої системи;

— будь-яка система має ієрархічну структуру, елементами і зв'язками якої не можна нехтувати без достатніх підстав;
— при аналізі системи необхідний облік зовнішніх і внутрішніх факторів, що впливають, прийняття рішень на основі частини з них без розгляду інших може привести до невірних результатів;
— властивості системи перевищують суму властивостей її елементів за рахунок якісно нових властивостей, відсутніх у її елементів — системних властивостей.

Ефективність реалізації системного підходу на практиці залежить від уміння фахівця виявляти і об'єктивно аналізувати все різноманіття факторів і зв'язків досить складного об'єкта дослідження, яким є, наприклад, організація як об'єкт захисту.

Необхідною умовою такого вміння є наявність у фахівця так званого системного мислення, що формується в результаті відповідного навчання та практики вирішення завдань, що слабо формалізуються.

Системне мислення [systems thinking] — це форма мислення, що характеризує здатність людини на несвідомому рівні вирішувати завдання дедуктивними методами. Ці методи стосовно до технічного захисту інформації передбачають:

— чітку постановку задачі, що включає визначення тематичних питань інформації та її джерел як об'єктів захисту, виявлення загроз цій інформації та формулювання цілей і завдань захисту інформації;
— розробку принципів і шляхів вирішення завдання;
— розробку методів вирішення завдань;
— створення програмного, технічного та методичного забезпечення вирішення завдань.

Системне мислення — це найважливіша якість не тільки фахівця із захисту інформації, а й будь-якого організатора і керівника. Якщо керівник не може швидко виявити фактори, що впливають на те чи інше рішення, і оцінити їх вагу, то невраховані або необґрунтовано відкинуті фактори постійно будуть про себе нагадувати. Такий керівник перетворюється на борця з ним же створюваними проблемами.

Якщо системний підхід характеризує концептуальні погляди на шляхи вирішення завдань, що слабо формалізуються, то основу їх вирішення становить системний аналіз.

Системний аналіз [system analysis] — 1) Аналіз об'єкта дослідження як сукупності елементів, що утворюють систему. У наукових дослідженнях він передбачає оцінку поведінки об'єкта як системи з усіма факторами, які впливають на його функціонування. Системний аналіз можна здійсню-

вати у відповідності до етапів системного аналізу. Кінцевим результатом системного аналізу є побудова моделі системи і розробка пропозицій з її удосконалення або зміни. 2) Аналіз призначення системи, яку передбачається проектувати, і встановлення множини вимог, яким вона повинна відповідати. Єдиної методики системного аналізу у наукових дослідженнях поки що немає. У практиці досліджень він застосовується з використанням таких методик:

- процедур теорії дослідження операцій, яка дає змогу дати кількісну оцінку об'єктам дослідження;
- аналізу систем дослідження об'єктів в умовах невизначеності;
- системотехніки, яка включає проектування і синтез складних систем у процесі дослідження їхнього функціонування.

Відповідно до вимог системного підходу сукупність взаємопов'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації, утворює систему захисту інформації.

Такими елементами є люди, інженерні конструкції і технічні засоби, що забезпечують захист інформації незалежно від їх приналежності до інших систем.

Ядро системи захисту утворюють сили і засоби, основними функціями яких є забезпечення інформаційної безпеки. Однак вони становлять лише частину сил і засобів системи захисту інформації.

Наприклад, в систему захисту інформації входять не тільки структурні підрозділи (служба безпеки, відділ режиму і секретності, 1-й відділ тощо), призначені для захисту інформації, але й всі співробітники організації, зобов'язані в міру своєї відповідальності забезпечувати захист інформації. Отже, вони також є елементами системи захисту інформації організації. І якщо який-небудь співробітник організації порушить правила поводження з секретними документами, то можливий величезний збиток, незважаючи на бездоганну роботу інших елементів системи захисту.

Отже, структура (елементи та їх взаємозв'язок) системи захисту інформації держави, відомства, організації пронизує структуру держави, відомства, організації.

1.2. Цілі, завдання і ресурси системи захисту інформації

Цілі являють собою очікувані результати функціонування системи захисту інформації, а завдання те, що треба зробити для того, щоб система могла забезпечити досягнення поставлених цілей (рис. 1.2) [130].

Можливість вирішення завдань залежить від ресурсу, що виділяється на захист інформації.

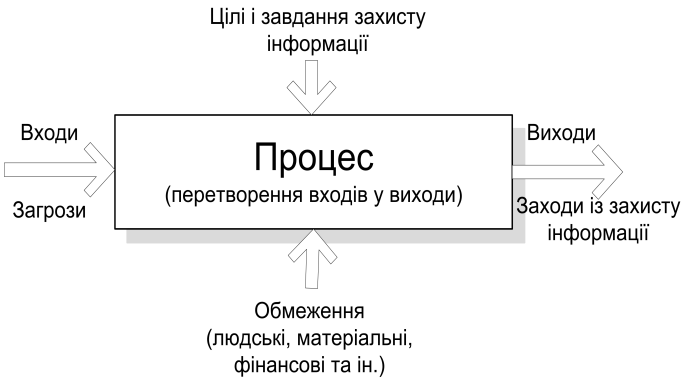

Рис. 1.2. Схематичне зображення системи захисту інформації

Ресурс включає в себе людей, що вирішують завдання захисту інформації, фінансові, технічні та інші засоби, що витрачаються на захист інформації.

Входами системи захисту інформації є загрози інформації, а виходами — заходи, які треба застосувати для запобігання реалізації загроз або зниження їх до допустимого рівня.

Нарешті, заходи, дії і технології, що визначають заходи захисту, відповідні загрозам, утворюють процес.

Основною метою технічного захисту інформації є забезпечення її безпеки, при якій ризик змінювання, знищення або розкрадання інформації не перевищує допустимого значення (рис. 1.3) [31].

Ризик [risk] характеризується ймовірністю реалізації загроз і залежить від ресурсу — прямих витрат на захист інформації. Сума прямих витрат на захист інформації і непрямих витрат, що відповідають збитку від реалізації загроз, визначає витрати на інформацію. Значення прямих витрат, при яких сумарні витрати на інформацію мінімізуються, утворюють область раціональної захисту інформації. Для оцінки ризику необхідно визначити джерела інформації та її вартість, загрози її безпеці і можливість (ймовірність) їх реалізації.

Завдання технічного захисту інформації визначають те, що треба виконати з урахуванням даного ресурсу для запобігання (нейтралізації) конкретних загроз в інтересах поставлених цілей.

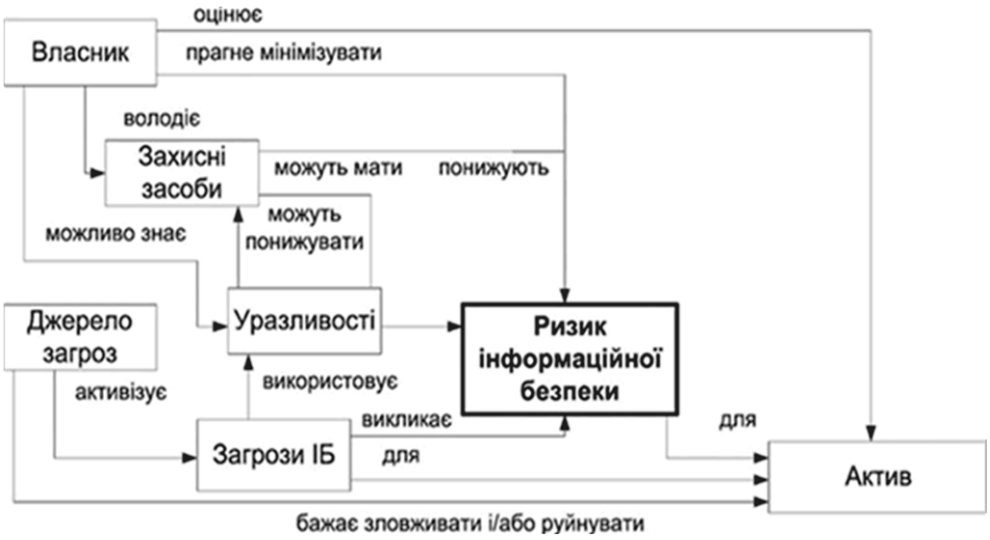

Рис. 1.3. Взаємозв'язок основних понять інформаційної безпеки

1.3. Загрози безпеці інформації і засоби щодо їх попередження

1.3.1. Основні властивості інформації як предмета захисту

Доступність інформації

Доступність інформації (даних) [availability of information] — це можливість використання інформації (даних), коли в цьому виникає необхідність (рис. 15.1). Доступність також характеризує працездатність інформаційної системи [3–5; 130].

Інформація доступна, коли вона міститься на матеріальному носії. До носіїв інформації (даних) [data medium] відносяться матеріальні об'єкти, які забезпечують запис, зберігання і передавання інформації у просторі і часі. Носіями інформації можуть бути:

— люди;
— матеріальні тіла (макрочастки);
— поля (випромінювання);
— елементарні частки (мікрочастки).

Так як за допомогою матеріальних засобів можна захищати тільки матеріальний об'єкт, то об'єктами захисту є матеріальні носії інформації. Розрізняють носії — джерела інформації, носії — переносники інформації та носії — одержувачі інформації.